Statistical-based SIP Traffic modeling scheme for Internet Telephony Service

Joon Heo, Tetsuya Kusumoto, Eric Chen

NTT Information Sharing Platform Laboratories, NTT Corporation

1. Introduction

An Internet telephony service which uses an IP packet network to transmit multimedia data is more advantageous compared with a public switched telephone network (PSTN) service. For these reasons, Internet Telephony users are rapidly increasing; it follows that a quantity of traffic and security vulnerabilities are also increasing. In this sense, network engineers should detect and prevent abnormal traffic to manage networks efficiently and securely. Compared with IP data networks, VoIP networks are more vulnerable since this service is supported by an application layer protocol such as Session Initiation Protocol (SIP). Consequently, it is important to analyze the traffic in VoIP networks; it is also useful for detecting the possibility of attacks using analysis results of traffic pattern. In the past researches which deal with abnormal traffic detection in VoIP network, such features are not considered seriously; for this reason, we propose statistical analysis method considering such features.

2. Proposed Modeling scheme and simulation

As we have noticed, an abnormal traffic can be included in normal traffic by various flooding type attacks. In this situation, we need to find a modeling value and boundary of normal traffic. In addition, we need to continuously update such a modeling value. The overall process of the proposed modeling method is shown in Figure 1 and Figure 2.

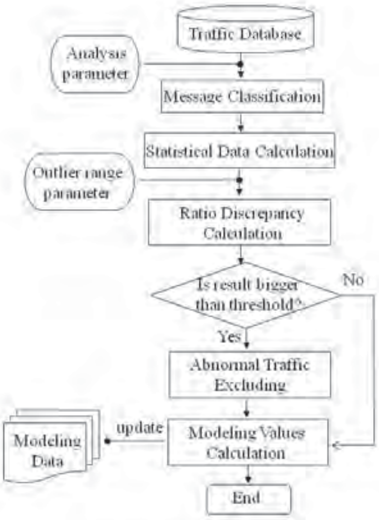

Traffic Database
Analysis parameter
Message Classification
Statistical Data Calculation
Outlier range parameter
Ratio Discrepancy Calculation
Is result bigger than threshold?
No
Yes
Abnormal Traffic Excluding
Modeling Data
update
Modeling Values Calculation
End

Figure 1. Overall process of modeling method

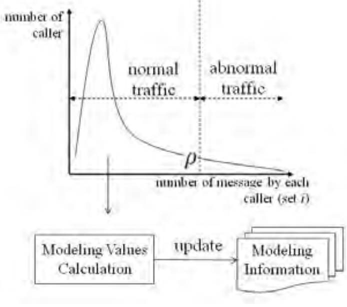
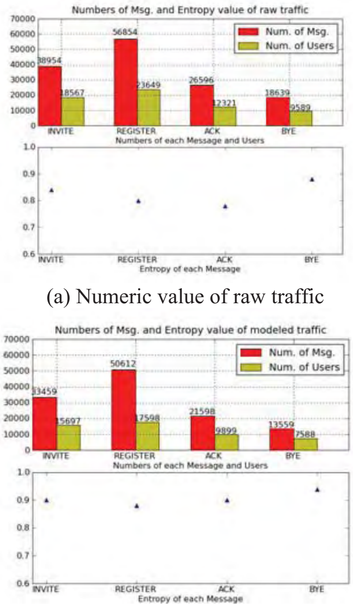


Figure 2. Concept of modeling information update

This process can be divided three steps. First step is classification and distribution calculation of each SIP message; second step is abnormal traffic decision and last step is excluding abnormal and modeling information update (as shown in Figure2). To compare modeling result, we analyzed SIP traffic obtained from experiment using the proposed module during few minutes and the results are shown in Figure 3-(a) and 3-(b).



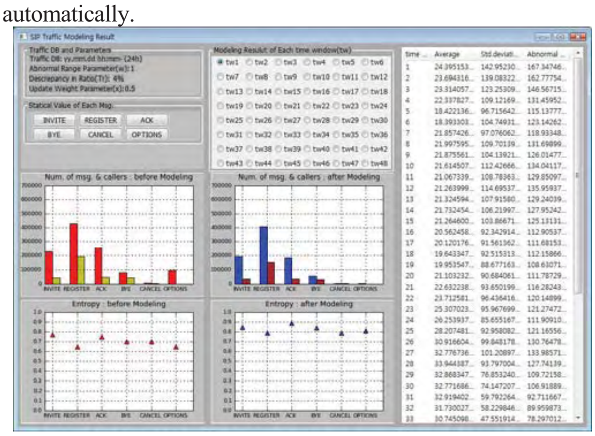
(a) Numeric value of raw traffic

(b) Numeric value after modeling

Figure 3. Comparison between raw traffic and modeled traffic

3. Implementation Result

To apply proposed modeling scheme into real service, we implemented prototype as shown in Figure4; this result was made by experiment data. We divided 1 day as 48 windows and this module can calculate statistical values (average, standard deviation and abnormal point), numeric information (number of message and number of callers) and entropy values of each SIP message. Also such modeled information can be updated automatically.


SIP Traffic Modeling Result
Statical Value of Each Msg.
INVITE
REGISTER
ACK
BYE
CANCEL
OPTIONS
Modeling Result of Each time window(tw)
● tw1 ○ tw2 ○ tw3 ○ tw4 ○ tw5 ○ tw6
○ tw7 ○ tw8 ○ tw9 ○ tw10 ○ tw11 ○ tw12
○ tw13 ○ tw14 ○ tw15 ○ tw16 ○ tw17 ○ tw18
○ tw19 ○ tw20 ○ tw21 ○ tw22 ○ tw23 ○ tw24
○ tw25 ○ tw26 ○ tw27 ○ tw28 ○ tw29 ○ tw30
○ tw31 ○ tw32 ○ tw33 ○ tw34 ○ tw35 ○ tw36
○ tw37 ○ tw38 ○ tw39 ○ tw40 ○ tw41 ○ tw42
○ tw43 ○ tw44 ○ tw45 ○ tw46 ○ tw47 ○ tw48
Num. of msg. & callers : before Modeling
Num. of msg. & callers : after Modeling
Entropy : before Modeling
Entropy : after Modeling
INVITE REGISTER ACK BYE CANCEL OPTIONS

Traffic DB and Parameters
Traffic DB: yy.mm.dd hh:mm~(24h)
Abnormal Range Parameter(w):1
Descrepancy in Ratio(Tr): 4%
Update Weight Parameter(x):0.5

time ...	Average	Std deviati...	Abnormal ...
1	24.395153...	142.95230...	167.34746...
2	23.694316...	139.08322...	162.77754...
3	23.314057...	123.25309...	146.56715...
4	22.337827...	109.12169...	131.45952...
5	18.422136...	96.715642...	115.13777...
6	18.393303...	104.74931...	123.14262...
7	21.857426...	97.076062...	118.93348...
8	21.997595...	109.70139...	131.69899...
9	21.875561...	104.13921...	126.01477...
10	21.614507...	112.42666...	134.04117...
11	21.067339...	108.78363...	129.85097...
12	21.263999...	114.69537...	135.95937...
13	21.324594...	107.91580...	129.24039...
14	21.732454...	106.21997...	127.95242...
15	21.264600...	103.86671...	125.13131...
16	20.562458...	92.342914...	112.90537...
17	20.120176...	91.561362...	111.68153...
18	19.643347...	92.515313...	112.15866...
19	19.953547...	88.677163...	108.63071...
20	21.103232...	90.684061...	111.78729...
21	22.632238...	93.650199...	116.28243...
22	23.712581...	96.436416...	120.14899...
23	25.307023...	95.967699...	121.27472...
24	26.253937...	85.655167...	111.90910...
25	28.207481...	92.958082...	121.16556...
26	30.916604...	99.848178...	130.76478...
27	32.776736...	101.20897...	133.98571...
28	33.944187...	93.797004...	127.74139...
29	32.868347...	76.853240...	109.72158...
30	32.771686...	74.147207...	106.91889...
31	32.919402...	59.792264...	92.711667...
32	31.730027...	58.229846...	89.959873...
33	30.745098...	47.551914...	78.297012...

Figure 4.GUI and modeling results of implemented prototype

In this work, we will develop SIP traffic analysis solution including modeling process, analysis, abnormal pattern classification and attack detection scheme for real Internet Telephony service. As the ongoing work, we are implementing the SIP traffic analysis function.